

ABSTRACT OF THE DISCLOSURE

Safe exceptions detect and intervene in a malicious attack against an application or system component, even in the presence of a coding flaw such as a buffer overrun. A list of all the exception handlers in an image (e.g., a DLL or EXE) is desirably created. When loading the image into a process, the operating system loader finds and stores a reference to this list. When a subsequent attack targets exception handling by creating an attacker provided exception handler, the new attacker provided exception handler is compared to a list of the real exception handlers. The list of real exception handlers is stored in memory, and desirably cannot be modified. In particular, when an exception occurs, the operating system finds the proper exception handler from information on the stack (this may be under attack, so the information is not trusted) and compares it to the previously created read-only reference list. If the exception handler that has occurred is found on the reference list, the exception handler is allowed to execute. Otherwise, the operating system assumes the application is under attack and terminates the process' execution.